UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/880,231	06/12/2001	Ron Karim	15437-0508	5058

29989   7590   08/10/2004

HICKMAN PALERMO TRUONG & BECKER, LLP
1600 WILLOW STREET
SAN JOSE, CA 95125

EXAMINER
WU, QING YUAN

ART UNIT	PAPER NUMBER
2127	

DATE MAILED: 08/10/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

	Application No.	Applicant(s)
Office Action Summary	09/880,231	KARIM, RON
	Examiner	Art Unit	
	Qing-Yuan Wu	2127	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *6/7/2002*.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-32* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-32* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage
      application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.

5)☐ Notice of Informal Patent Application (PTO-152)

6)☐ Other: _____.

DETAILED ACTION

1.   Claims 1-32 are pending in the application.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the

basis for the rejections under this section made in this Office action:

> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on
> sale in this country, more than one year prior to the date of application for patent in the United States.

2.   Claims 1-2, 4, 7-8, 10, 12-18, 20, 23-24, 26, and 28-32 are rejected under 35

U.S.C. 102(b) as being anticipated by Schnurer et al (U.S. Patent 5,842,002).

3.   As to claims 1 and 17, Schnurer et al teach the invention as claimed including a

computer-implemented method for executing an untrusted program [abstract, lines 1-2],

comprising:

establishing a limited environment, said limited environment comprising at least one

mock resource [col. 4, lines 16-20, 22-26, 47-49; col. 7, lines 3-8];

executing at least a portion of an untrusted program within said limited environment

[col.7, lines 5-12]; and examining said limited environment after execution of at least

said portion of said untrusted program to check for undesirable behavior exhibited by

said untrusted program [col. 4, lines 32-36; col. 7, lines 12-15; 48, 50, 52, Fig. 1].

4.   As to claim 2, Schnurer et al teach the invention as claimed including where said limited

environment precludes access to actual resources, which if altered or accessed by said untrusted

program, may lead to undesirable consequences [abstract; col. 5, lines 5-10; col. 7, lines 15-18].

5.   As to claim 4, Schnurer et al teach the invention as claimed including wherein examining

said mock environment comprises: determining whether said mock resource has been deleted

[col. 4, lines 37-39; col. 7, lines 12-15].

6.   As to claim 7, Schnurer et al teach the invention as claimed including wherein examining

said mock environment comprises: determining whether said mock resource has been altered

[col. 7, line 48 to col. 8, line 26].

7.   As to claim 8, Schnurer et al teach the invention as claimed including wherein said mock

resource has a parameter associated therewith which changes when said mock resource is altered,

and wherein determining whether said mock resource has been altered, comprises:

determining whether said parameter has changed [col. 7, line 48 to col. 8, line 26].

8.   As to claim 10, Schnurer et al teach the invention as claimed including wherein

examining said mock environment comprises:

determining whether said mock resource has been accessed [col. 7, line 48 to col. 8, line 26].

9.   As to claim 12, Schnurer et al teach the invention as claimed including providing

information indicating behavior exhibited by said untrusted program [col. 7, line 25 to col. 8, line

26].

10.   As to claims 13 and 14, Schnurer et al teach the invention as claimed including wherein

said information comprises indications of undesirable behavior exhibited by said untrusted

program [col. 7, lines 48-52], and in response to a determination that said untrusted program has

exhibited undesirable behavior, taking corrective action [col. 8, lines 27-35; 52, Fig. 1].

11.   As to claims 15 and 16, Schnurer et al teach the invention as claimed including wherein

taking corrective action comprises: deleting said untrusted program and warning to a user [col. 8,

lines 27-35; 52, Fig. 1].

12.   As to claims 18, 20, 23-24, 26, and 28-32, these are system claims that correspond to the

method claims 2, 4, 7-8, 10, and 12-16. Therefore, they are rejected for the same reason as

claims 2, 4, 7-8, 10, and 12-16 above.

Claim Rejections - 35 USC § 103

13.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

14.   Claims 3, 5-6, 9, 11, 19, 21-22, 25, and 27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schnurer et al (U.S. Patent 5,842,002).

15.   As to claims 3 and 19, Schnurer et al do not teach a limited environment comprises a shell in a UNIX operating system environment. However, Schnurer et al disclose different operating systems [col. 3, lines 59-66].

It would have been obvious to one of ordinary skill in the art at the time of the invention was made to have included a UNIX operating system in Schnurer et al's system because UNIX is well known to be a powerful operating system.

16.   As to claims 5-6 and 9, Schnurer et al teach the invention substantially as claimed in claim 1. Schnurer et al did not specifically teach the step of determining whether said mock resource has been renamed and moved. However, Schnurer et al disclosed that his system can detect any malicious act by the virus, including the activities of changing the FAT table and changing of the error checking algorithm [col. 7, lines 59-60; col. 8, lines 25-26; col. 4, lines 37-39].

17.   It would have been obvious to one of an ordinary skill in the art at the time the invention was made, to have recognized that common viral activities or critical behaviors exhibited by

viruses would have included the renaming and moving of system resources as being considered and implemented in Schnurer et al's method of virus detection.

18.   As to claim 11, Schnurer et al teach the invention substantially as claimed in claim 1, including wherein said mock resource contains one or more sets of content, wherein said untrusted program executes in a particular portion of memory, and wherein determining whether said mock resource has been accessed comprises:

searching said particular portion of said memory for at least one of said one or more sets of content. Is known in the art that when a file gets accessed or altered, traces of the contents being accessed is located in the memory (Schnurer et al disclosed the determination of potential viral activities by examining "if anything within the environment changes…" col. 7, line 48 to col. 8, line 26.)

19.   As to claims 21-22, 25, and 27, these are system claims that correspond to the method claims 5-6, 9, and 11. Therefore, they are rejected for the same reason as claims 5-6, 9, and 11 above.

20.   The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

U.S. Patent No. 6,151,618 to Wahbe et al, U.S. Patent No. 5,826,013, 5,696,822 and 6,067,410 to Nachenberg teach executing untrusted programs in a limited environment.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Qing-Yuan Wu whose telephone number is (703) 305-8788. The examiner can normally be reached on 8:30am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Meng-Ai An can be reached on (703) 305-9678. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Qing-Yuan Wu

Examiner

Art Unit 2127

MENG-AL T. AN
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100